CLAIMS

What is claimed is:

1. A method for providing virus protection of computer system comprising a central processing unit, a hard disk, a nonvolatile random access memory, an Extensible Firmware Interface, and a basic input and output system, the method comprising the steps of:

modifying a command shell of the Extensible Firmware Interface to include a command that operates to copy the boot sector of the hard disk to the nonvolatile random access memory;

storing the modified Extensible Firmware Interface in the nonvolatile random access memory;

when the computer system is initialized, copying a boot sector of the hard disk to the nonvolatile random access memory;

reading back the boot sector of the hard disk from the nonvolatile random access memory on each boot to bypass boot sector access of the hard disk during system initialization.

2. The method recited in Claim 1 which comprises software.

3. The method recited in Claim 1 which comprises firmware.

4. The method recited in Claim 1 further comprising the step of:

adding a field to a BIOS SETUP portion of the BIOS, that allows a user to enable or disable reading the boot record from nonvolatile random access memory on boot;

running the BIOS SETUP portion of the BIOS; and

enabling or disabling reading the boot record from nonvolatile random access memory on boot.

5. The method recited in Claim 1 further comprising the step of:

further modifying the command shell of the Extensible Firmware Interface to include a command a security signature input field;

during execution of the Extensible Firmware Interface, displaying the security signature input field to a user; and

inputting the required signature prior to updating the stored boot sector.

6. The method recited in Claim 4 further comprising the step of:

further modifying the command shell of the Extensible Firmware Interface to include a command a security signature input field;

during execution of the Extensible Firmware Interface, displaying the security signature input field to a user; and

inputting the required signature prior to updating the stored boot sector.

7. The method recited in Claim 1 wherein the modified Extensible Firmware Interface is stored in a read-only-memory.

8. The method recited in Claim 1 wherein the modified Extensible Firmware Interface is stored in a flash memory.